UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

PATI SPRINGMEYER, an individual and Nevada Resident, and JOE LOPEZ, an individual and California Resident, on behalf of themselves and all others similarly situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC., a Montgomery County, Maryland Resident,

Defendant.

Case No. 8:20-CV-00867-PWG

Judge Paul W. Grimm

PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

MURPHY, FALCON & MURPHY, P.A.
William H. Murphy III, Esq. (Bar No. 30126)
hassan.murphy@murphyfalcon.com
One South Street, 23rd Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen Hanson Riebel (*pro hac vice*)
khriebel@locklaw.com
Kate M. Baxter-Kauf (*pro hac vice*)
kmbaxter-kauf@locklaw.com
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

GLANCY, PRONGAY & MURRAY
Brian Murray
BMurray@Glancylaw.com
230 Park Avenue, Suite 530
New York, NY 10169
Telephone: (212) 682-5340
Facsimile: (212) 884-0988

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (*pro hac vice*)
jyanchunis@ForThePeople.com
Jean S. Martin (*pro hac vice*)
jeanmartin@ForThePeople.com
Ryan J. McGee (*pro hac vice*)
rmcgee@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

TOSTRUD LAW GROUP, P.C.
Jon A. Tostrud (*pro hac vice*)
jtostrud@tostrudlaw.com
Anthony M. Carter (*pro hac vice*)
acarter@tostrudlaw.com
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Facsimile: (310) 278-2640

Attorneys for Plaintiffs

Table of Contents

Table of Authorities

Cases

Statutes

INTRODUCTION

Following yet another massive security breach where Marriott International, Inc. ("Marriott") acknowledged that the login credentials of two of its employees had been compromised, and "an unexpected amount of guest information" had been improperly accessed (the "Breach"), Plaintiffs, Pati Springmeyer and Joe Lopez, brought this class action lawsuit to seek damages and injunctive relief on behalf of aggrieved consumers. Marriott now seeks to eschew its clear obligations to protect consumers' personal identifiable information ("PII") via its Motion to Dismiss (Doc. 40-1) (the "Motion" or "MTD"), arguing Plaintiffs have suffered no damages, have no legal recourse, and should instead be left to navigate the mess Marriott created through its poor, lax, and ineffective data and cyber security functions. This Court should deny Marriott's Motion outright and permit Plaintiffs to pursue their well-pled allegations.

BACKGROUND

Plaintiffs Springmeyer and Lopez allege, via the Amended Class Action Complaint (Doc. 36)[1] that Marriott, one of the largest hotel chains in the world, collects profiles containing extensive personal information for prospective and actual guests reserving and booking rooms at a Marriott property, and requires that guests provide this information as a condition of staying at a Marriott property. ¶¶ 2, 26. On March 31, 2020, Marriott announced the Data Breach at issue in this litigation, and which occurred when "the login credentials of two of its employees had been compromised and 'an unexpected amount of guest information' had been improperly accessed as early as mid-January 2020." ¶¶ 3, 23–24. Marriott announced that:

> The compromised guest data included: Contact Details (e.g., name, mailing address, email address, and phone number); Loyalty Account Information (e.g., account number and points balance, but not passwords); Additional Personal Details (e.g., company, gender, and birthday day and month); Partnerships and

[1] All references to allegations in the Amended Class Action Complaint are hereinafter referred to by paragraph as "¶ __."

> Affiliations (e.g., linked airline loyalty programs and numbers); and Preferences (e.g., stay/room preferences and language preference) (hereinafter, the "PII").

¶ 3. This announcement came on the heels of a *different*, previous breach that Marriott announced in November 2018, where personal information of 500 million Marriott guests was exposed "due to a flaw in its reservation and database systems." ¶ 4. The Data Breach was a "direct result of Marriott's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its guests PII," failures for which Marriott was entirely on notice for and aware of, given its massive breach announced less than eighteen months prior. ¶¶ 5, 36. Marriott's failure to implement and follow even basic security procedures has left Plaintiffs and Class Members' PII in the hand of thieves, and they have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud." ¶¶ 7, 42–47, 54–63.

Both Plaintiff Springmeyer and Plaintiff Lopez were notified that their PII had been compromised and "accessed without authorization" during the Data Breach. ¶¶ 11, 18. As a result of the Data Breach, Ms. Springmeyer purchased credit monitoring services at an annual cost of $159.96, and spent valuable time to monitor accounts in an effort to detect and prevent misuse of her PII, and continues to spend valuable time to monitor her accounts to detect and prevent misuse and to protect the integrity of her PII. ¶¶ 12–14. Similarly, as a result of the breach, Mr. Lopez spent valuable time to monitor accounts in an effort to detect and prevent misuse of his PII and continues to spend valuable time to monitor his accounts to detect and prevent misuse and to protect the integrity of his PII. ¶¶ 18–19. Both Plaintiffs suffered actual injury from having their PII exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Marriott for its services which they would not have, had Marriott disclosed that it lacked data and cyber security practices adequate to safeguard consumers' PII from theft; (b) damages to and

diminution in the value of their PII—a form of intangible property that Plaintiffs entrusted to Marriott as a condition for hotel services; (c) imminent and impending injury arising from the increased risk of fraud and identity theft; and (d) that Plaintiffs will continue to be at a heightened risk of fraud and identity theft, and their attendant damages, for years to come. ¶¶ 15–16, 20–21. These injuries were similarly felt by Class Members. ¶¶ 64–70.

As a result, Plaintiffs allege claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, declaratory judgment, and seek to certify a Nationwide Class, as well as alleging California- and Nevada-state-based claims for the respective subclasses. ¶ 8, 75–192. Plaintiffs also seek to compel Marriott to adopt reasonably sufficient security practices to safeguard guest PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future. *See* ¶¶ 8, 147–154, Prayer for Relief.

ARGUMENT

I. Plaintiffs Have Article III Standing

In order to have standing, Plaintiff must allege a concrete injury which is real and not abstract. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). The size of the injury is immaterial. A small injury or identifiable trifle is sufficient to confer standing on a plaintiff. The question is whether each Plaintiff here has a direct stake in this litigation or is merely "a person with a mere interest in the problem."[2] *U.S. v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 690 (1973). The direct harm need not be monetary harm to have a concrete injury for Article III standing. *Id*. at 686.

[2] "To draw on proximate cause imagery, one way to look at it is whether the plaintiff is in the "zone of harm," even though proximate cause is not a requirement of Article III standing, *Lexmark Int'l. v. Static Control Components*, 572 U.S. 118, 134 n.6 (2014).

A. Plaintiffs Have Alleged an Injury-In-Fact

"To establish injury-in-fact, a plaintiff must show that he or she suffered "'an invasion of legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural of hypothetical'." *Spokeo*, 136 S. Ct. at 1548. An injury may include mitigation-related expenses "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Clapper v. Amnesty Int'l. v. USA*, 568 U.S. 398, 414 n.5 (2013). To invoke federal subject matter jurisdiction and have Article III standing, a plaintiff must allege 1) an injury-in-fact; 2) that is fairly traceable to defendant's conduct; and 3) that is likely to be redressed by a favorable decision. *Spokeo*, 136 S. Ct. at 1540. Defendant only challenges the first and second prongs under *Spokeo*.

The two controlling Fourth Circuit cases are *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), and *Hutton v. Nat'l Board of Examiners in Optometry*, 892 F.3d 613 (4th Cir. 2018). *Beck* is a data security case, while *Hutton* is a data breach case, closer in type to the case at bar. This Court had the benefit of both decisions when it decided the 2019 Marriott data breach case. *In re Marriott Int'l. Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020) ("*Marriott MDL*").

Defendant fails to recognize the critical distinction between *Beck* and *Hutton*. Unlike this case, which involves the deliberate targeting of login credentials and improper accessing of PII (a classic data breach), *Beck* involved lost or stolen materials that coincidentally contained PII. The motivations in *Beck* were unknown. 848 F.3d at 263. Even after discovery, on the summary judgment record the *Beck* plaintiffs could not show their PII was compromised in any way. It is therefore not surprising the Fourth Circuit found the *Beck* plaintiffs' "contention of an enhanced risk of future identity theft [is] too speculative." *Id*. at 274. *Beck* was no different than *Randolph*

v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007), where a laptop which was stolen by a burglar happened to contain PII. *Beck* and *Randolph* are theft cases, not data breach cases.

Hutton identified the difference between a common theft and a targeted data breach. The Fourth Circuit in *Hutton*, distinguishing *Beck*, stated "there was no evidence that the thief even stole the laptop with the intent to steal private information." 892 F.3d at 622. Even so, *Hutton* was not a "classic" data breach along the lines of Yahoo, Equifax, Marriott in 2019, or Marriott in this case, to name a few, where there was a deliberate targeting of information, a "hack," and a confession by the defendant that hackers exploited poor security measures. In *Hutton*, a group of optometrists realized their PII was stolen and deduced the defendant was hacked (the defendant never admitted to the hack). *Id*. Even so, the *Hutton* case, combined with this Court's previous *Marriott MDL* decision, and out of Circuit cases, provides plenty of authority to conclude that plaintiffs have standing here.

The *Hutton* court stated that *Clapper* "recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists." *Id*. It went on to state "[b]ecause the injuries alleged by the plaintiffs are not speculative, the costs of mitigating measures to safeguard against future identity theft support the other allegations and together readily show sufficient injury-in-fact to satisfy the first element of the standing to sue analysis." *Id*. In other words, when it is clear why and how the PII at issue was compromised, and it is reasonable to conclude a bad actor was involved, injury-in-fact follows logically. *Id.*; *see also Remijas v. Neiman Marcus Group*, 794 F.3d 688, 693 (7th Cir. 2015) (concluding that the reason hackers break into databases, *inter alia*, is to assume others' identities).

B. This Court Previously Found Standing under Substantially Similar Facts Involving the Same Defendant

This Court, in *Marriott MDL*, recognized that in *Beck* "there was no indication that the laptop or the boxes . . . were stolen for the purpose of identity theft in the first place or that any plaintiffs were victims of identity theft." 440 F. Supp. 3d at 457. In other words, a chain of assumptions, guesses, and inferences would have to be made in *Beck* in order to find that anyone's PII was at risk. Therefore "because the threat of identity theft was too speculative," the cost of mitigating the speculative harm was too attenuated to establish injury-in-fact. *Id*. at 458. This Court then examined the *Hutton* case and succinctly summarized the difference:

> [I]n *Beck* "there was no evidence that the thief even stole the laptop with the intent to steal private information . . . the [*Hutton*] plaintiffs allege that their data has been stolen, accessed, and used in a fraudulent manner." 882 F.3d at 622. Finally, the Fourth Circuit held that given the non-speculative nature of these alleged injuries, the plaintiffs' out-of-pocket costs and time spent to mitigate the harms also constituted injury-in-fact.

Id at 459. This Court took pains to differentiate the *Marriott MDL*'s targeted breach (as exists here) from *Beck*, lacking targeting allegations, or *Hutton*, lacking public acknowledgment.

Defendant's claim that this Court only departed from the holding of *Chambliss v. Carefirst, Inc*., 189 F. Supp. 3d. 524 (D. Md. 2016), in *Marriott MDL* because the Court found "plaintiffs could proceed if they showed harm to 'the economic benefit[s] consumer derives from being able to [make] puchase[s] remotely and without the need to pay in cash or check'." MTD at 7 (quoting *Marriott MDL*, 440 F. Supp. 3d at 462). But whereas the subquote from the brief is in the opinion, the windup to this clause is nowhere to be found. This Court did not state the plaintiffs could only proceed if they could show harm to the "economic benefit." Quite the opposite. The Court took judicial notice of some facts and applied common sense to others to come to the unremarkable conclusion that when PII is compromised, its value is diminished.

C. The Facts Of This Case Evince Injury And Standing

1. Increased risk of identity theft is cognizable injury.

Defendant cagily tries to portray the Breach as simply two Marriott employees accessing customer PII. MTD at 9 (compromised data was by "hotel employees who, generally, have access to such data"). This is, at best, an optimistic spin on the facts and at worst complete dissembling. The notification by Marriott states "we identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees." ¶ 24. Either a bad actor hacked into Marriott's database, or a Marriott employee far exceeded permissions and accessed PII without consent. Plaintiffs unquestionably have been harmed and are at an increased risk of identity theft. *See, e.g.*, *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017) ("No long sequences of uncertain contingencies involving multiple independent actors has to occur before the plaintiff in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.").

2. Time and effort spent protecting PII is cognizable injury.

Time and money spent mitigating harm from a data breach constitutes injury-in-fact. *Marriott MDL*, 440 F. Supp. 3d at 460. As this Court stated, although the speculation that there was a theft and that the theft may cause harm was too attenuated in *Beck*, in *Hutton*, where the inference of a data breach was stronger but still unadmitted, the time and cost of mitigation was sufficiently non-speculative to constitute injury-in-fact. Here, the fact that Marriott admitted the Breach, the targeting and compromise of Plaintiffs' and Class Members' PII is not in doubt, and injury-in-fact is therefore sufficiently non-speculative to establish standing.

Defendant attempts to make much of the fact that the compromised PII in this case involves "only" name, address, email address, phone number, Marriott account number and balance, employer, gender, birthday, any linked airline loyalty numbers, and Marriott room preferences.

Defendant would have this Court believe that in the absence of divulging social security or credit card numbers, all information can be left unguarded and freely spread to the world without penalty. This defies common sense, as many courts have recognized. For instance, in *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 691 (N.D. Cal. 2019), no social security or credit card numbers were taken, but the Court recognized that birthdays, hometowns, and gender are long-term sensitive information. While credit cards may be cancelled,[3] PII is permanent. *Id.*

3. Lost benefit of the bargain is cognizable injury.

This Court, again in the *Marriott MDL*, addressed the issue of whether the failure to receive the benefit of the bargain constitutes injury-in-fact by surveying all available cases and found that failure to receive the benefit of the bargain regarding data security does constitute injury-in-fact. 440 F. Supp. 3d at 463. Following the Eighth Circuit[4] and cases within the Ninth Circuit,[5] this Court found sufficient allegations: (1) that an explicit or implicit contract for data security existed based on privacy statements; (2) that plaintiffs placed significant value on data security; and (3) that had plaintiffs known of Marriott's lax security practices, they would not have stayed at Marriott or would have paid less for their stays. *Id*. at 465–66. Here, Plaintiffs make similar allegations. Plaintiffs allege they placed value on data security, ¶ 140, that had they known the truth they would either not have stayed at Marriott or paid less for the privilege, ¶ 133, and that Marriott's privacy statements form an express or implied contract, ¶¶ 120–124.

Defendant also claims that without facts showing hotels give discounts to guests who raise data security concerns, there can be no benefit of the bargain losses. MTD at 9. This argument

[3] *See Rudolph v. Hudson's Bay Co*., 2019 WL 2023713 (S.D.N.Y. May 7, 2019) (no imminent harm from stolen credit card number when card was cancelled).
[4] *Carlsen v. Gamestop, Inc*., 833 F.3d 903 (8th Cir. 2016).
[5] *In re Yahoo! Inc. Customer Data Sec. Breach Litig*., 313 F. Supp. 3d 1113 (N.D. Cal. 2018); *In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953 (N.D. Cal. 2016).

misses the point. The point is not that a guest bargains at the Marriott front desk for a discount, but rather that a guest stays at a Marriott, relying on its reputation and privacy statement, rather than staying at the lower-priced motel, with a lesser reputation and perhaps no privacy statement.

4. Diminution in value or loss of PII is cognizable injury.

The Fourth Circuit has not opined on whether the loss of property value in PII constitutes a cognizable injury in data breach cases. However, this Court, in *Marriott MDL*, surveyed national cases on the issue before examining the issue in detail, plaintiffs alleged "Marriott recognizes the value of [PII] and collects it to better target customers and increase its profits." 440 F. Supp. 3d at 461. Plaintiffs make similar allegations here. ¶ 32. In *Marriott MDL,* this Court also found that PII is coveted and valuable on underground or black market, *id.* at 461, consistent with allegations in this case. *Cf* ¶¶ 46–47. This Court also found that PII has value in our digital economy and forms a part of most commercial transactions. 440 F. Supp. 3d at 462. Applying all these factors, this Court held the loss of property value when PII is purloined is an injury-in-fact. The similarity of the allegations warrants a similar conclusion here.

D. Plaintiffs' Injuries Are Fairly Traceable to Marriott's Conduct

Defendant makes little more than a token effort to argue Plaintiffs' injuries are not fairly traceable to the Breach. Defendant again trots out the fiction that the Breach was caused by a rogue employee doing his job. This tacitly proves Plaintiffs' case: if any Marriott employee can access any Marriott guest's PII at will, with no safeguards, this alone is *prima facie* evidence of negligent procedures which any "reasonable" procedure should prevent. Even absent credit card and social security numbers, a consumer's name, email address, and phone number are valuable information in the hands of a fraudster. *Bass v. Facebook*, 393 F. Supp. 3d 1024, 1034 (N.D. Cal. 2019). The risk of identity theft, time and effort spent protecting PII, the diminution of value of PII, and the loss of the benefit of the bargain are all directly traceable to the Breach and compromise of

Plaintiffs' PII—now in the hands of bad actors. As the *Bass* court pointed out, acts like these are not a random looting but a targeted attack with a purpose—identity theft. *Id*. at 1034–35.

E. Plaintiffs Have Standing to Pursue Injunctive Relief

Marriott's continued reliance on *Beck* with regard to Plaintiffs' claims for injunctive relief is misplaced. As argued above, the *Beck* court held that a chain of guesses, assumptions, and inferences were necessary to find that anyone's PII was at risk, and dismissed for lack of standing. *Supra* I.A–C; *Beck,* 848 F.3d at 277–78. Unsurprisingly, the *Beck* court also held that plaintiffs were not entitled to injunctive relief because the "most that can be reasonably inferred from the Plaintiffs' allegations regarding the likelihood of another data breach at [defendant] is that the Plaintiffs *could* be victimized by a future data breach. That alone is not enough." *Id.* at 277–78. Here, instead, Plaintiffs clearly plead that Marriott continues to possess consumers' PII, and has a demonstrated inability to prevent a data breach or stop it from continuing even after detection. ¶ 70. Marriott permitted two Russian franchise employees access to the guest information of approximately 5.2 million consumers, MTD at 1, many of whom have never stayed at that property or even visited that country. Therefore, it is not hypothetical or conjectural; instead, Plaintiffs face a continued threat that their PII, entrusted to Marriott, will continue to exist in an insecure environment. Plaintiffs have standing to pursue this relief.

II. Plaintiffs Have Sufficiently Pled their Claims

A. Common-law governance

1. Plaintiffs' tort claims are governed by Maryland law.

Marriott argues the rule of *lex loci delicti* governs Plaintiffs' tort claims, but contends the events giving rise to the tort action occurred in more than one state in conclusory form without any allegations or support. MTD at 12. This argument squarely belies Plaintiffs' well-pled Amended Complaint—Marriott's principal place of business is located in Bethesda, Maryland, and Maryland

is the "nerve center" of its business activities, including where its data and cyber security functions and major policy, financial, and legal decisions are made; Marriot's response to the Breach was made from Maryland; and Marriott's duties to Plaintiffs and Class Members emanated from Maryland. ¶¶ 89, 91, 92. The injuries to Plaintiffs and Class Members occurred from Marriott's "never center" in Bethesda, Maryland, and this Court should therefore apply Maryland law. *See, e.g., Tenax Corp. v. Tensar Corp.*, 1990 WL 152565, at *4 (D. Md. May 31, 1990) (discussing *lex loci delicti* rule and how injury occurs where the information is used or developed).

2. Plaintiffs' contract claims are governed by Maryland law.

Marriott argues on the one hand that no contract exists, MTD at 15–17, but then argues that any "alleged contract would have been accepted, and so 'made,' in Plaintiffs' home states." MTD at 12. Assuming *arguendo* that Marriott had not explicitly assented to the terms of the contract Plaintiffs seek to enforce, Marriott accepted the terms of the contract by accepting and storing Plaintiffs' and Class Members' PII. *See, e.g., Mogavero v. Silverstein*, 790 A.2d 43, 52–53 (Md. 2002) (a contract may be implied in fact where the conduct of the parties shows a meeting of the minds and mutual intent to contract). Here, Plaintiffs and Class Members provided their PII subject to Marriott's representations that the PII would be secure, and Marriott accepted that PII. *Harte-Hanks Direct Mktg./Baltimore, Inc. v. Varilease Tech. Fin. Grp., Inc.*, 299 F.Supp.2d 505, 518 (D. Md. 2004). Therefore, although Marriott disputes the formation of a contract, Marriott nevertheless accepted the PII and purported to protect that PII and, upon acceptance, Marriott assented to the contract in Maryland. Therefore, *lex loci contractus* inures to the benefit of Plaintiffs and Class Members, and their contract claims should be analyzed under the law of Maryland.

B. Negligence and Negligence *Per Se*

Negligence requires: 1) a duty owed to plaintiff; 2) breach of that duty; 3) a legally cognizable causal relationship between the breach of duty and the harm suffered; and 4) damages.

Casey v. Geek Squad Subsidiary Best Buy Stores, L.P., 823 F. Supp. 2d 334, 350 (D. Md. 2011).[6] Plaintiffs acknowledge California and Maryland do not recognize negligence *per se*, but instead treat a violation of a statutory standard as evidence of negligence, with a regulatory statute defining duty and breach. *Dent v. Nat'l Football League*, --- F.3d ---, 2020 WL 4558291, at *3 (9th Cir. Aug. 7, 2020); *Bray v. Marriott Int'l.*, 158 F. Supp. 3d 441, 444–45 (D. Md. 2016);[7] *see also Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.*, 125 Nev. 818, 828 (Nev. 2009).

The weight of legal authority holds that a company has a common law duty to protect personal private, sensitive information with which it is entrusted. *See, e.g.*, *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *7 (M.D. Fla. Jan. 27, 2020) (holding that company had duty to properly protect customer data due to knowledge of proliferated data breaches); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1321 (N.D. Ga. 2019) ("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information."); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (holding "the legal duty [to safeguard a consumer's confidential information entrusted to a commercial entity] is well supported by both common sense and California and Massachusetts law").[8]

---

[6] The same is true under California and Nevada law. *Paz v. California*, 22 Cal.4th 550, 559 (2001); *Sanchez ex rel. Sanchez*, 125 Nev. at 824.

[7] Under Maryland law, Plaintiffs concede dismissal of the negligence *per se* count is proper so long as Plaintiffs are permitted to use a violation of the statutory standard as evidence of negligence; however, should the Court apply California or Nevada law, the claim survives, as California and the FTC have passed laws regulating and defining duty and breach, discussed *infra*.

[8] California has specifically informed businesses that if they have or use a California resident's PII, they "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." *Cal. Civ. Code* §1798.81.5(b). Likewise, the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a similar duty of care across the United States. *Hameed-Bolden v. Forever 21 Retail Inc.*, 2018 WL 6802818, at *1, *4 (C.D. Cal. Oct. 1, 2018).

Marriott attempts to cast Plaintiffs' factual pleadings as conclusory and a "naked assertion" concerning how Marriott breached its duty to maintain the security of Plaintiffs' and Class Members' PII. MTD at 13. This is simply not true, as Marriott itself admitted that "an *unexpected* amount of guest information may have been accessed using the login credentials of two employees at a franchise property." ¶ 24. The number of impacted consumers is not trivial; at a minimum, some 5.2 million guests were notified that their PII had been compromised. ¶ 23. A reasonable conclusion drawn from this fact is that login credentials—from a franchise property located in a foreign country—were used to access the PII of millions of consumers in the United States, including Plaintiffs and Class Members. As discussed, *infra*, Marriott's representations leave two bleak certainties: either the credentials were misused by employees, or malicious actors hacked the credentials and pilfered consumers' PII. The suggestion that this Court "can have 'no idea how' Marriott allegedly breached" its duty to Plaintiffs and Class Members, MTD at 13, falls flat, and Marriott admits the "data was accessed *improperly* by franchise employees." MTD at 16, n.9.

Finally, for the reasons argued *supra*, I.B.1–4, Plaintiffs have alleged sufficient damages to survive a Rule 12(b)(6) challenge. Marriott contemptuously speculates "Springmeyer's spending was driven by litigation, not privacy concerns," MTD at 14, because Plaintiffs did not plead whether they visited Marriott's online self-service portal in the wake of the data breach. Plaintiffs bear no requirement to make such an allegation, have no obligation to accept the paltry credit monitoring services Marriott offered, and should never be compelled to provide additional information to Marriott's "online self-service portal" following notice that Marriott failed to protect the information it already had. If Marriott could not properly silo an employee's credentials, there is no guarantee Marriott would appropriately handle Plaintiffs' or Class Members' information submitted to this portal. Marriott's bombastic accusations aside, the Court should deny Marriott's Motion on the law. *See, e.g.*, *Marriott MDL*, 440 F. Supp. 3d at 494; *In re*

Equifax, 362 F. Supp. 3d at 1316; *Adkins*, 424 F. Supp. 3d at 691; *In re Arby's Rest. Grp. Inc. Litig.*, 2018 WL 2128441, at *11 n.12 (N.D. Ga. March 5, 2018); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017); *In re: Anthem*, 162 F. Supp. 3d at 994. These damages are fairly traceable to Marriott's conduct, the Breach, and would not have been otherwise incurred. *Ibid.*

Marriott argues the economic loss doctrine bars Plaintiffs' negligence claims. Again, Marriott misses the mark. The economic loss doctrine is designed to prevent tort and contract law from dissolving into one another, and Marriott here repeatedly eschews any contract. If there is no contract, the economic loss doctrine has no application. *UMG Recordings Inc. v. Global Eagle Entm't. Inc.*, 2015 WL 12746208, at *11 (C.D. Cal. Oct. 30, 2015). Indeed, under either Maryland or California law, this Court has held the economic loss doctrine has no application when a defendant breaches a legal duty independent of the contract—even when only economic loss ensues. *Pasternak & Fidis, P.C. v. Recall Total Info. Mgmt., Inc.*, 95 F. Supp. 3d 886, 900 (D. Md. 2015); *Jacques v. First Nat'l Bank of Md.*, 515 A.2d 756, 759–60 (1986); *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal.4th 979, 989 (2004); *In re: Equifax*, 362 F. Supp. 3d at 1320. Moreover, contrary to Marriott's Motion, Plaintiffs do allege a "special relationship." (¶ 98). Plaintiffs allege Marriott has a duty to continue to safeguard their PII even after the hotel stay or transaction has ended. ¶ 27. Finally, Plaintiffs' injuries were not "purely" economic harm—they suffered property damage in the form of diminished value of their PII. *See Arch Ins. Co. v. Costello Const. of Md., Inc.*, 2020 WL 1158776, at *3 (D. Md. March 9, 2020) (Chasanow, J.) (recognizing that "when negligence causes property damage, rather than purely economic harm, the economic loss doctrine does not apply *at all*.") Thus, even under Marriott's misreading of the Complaint and misapplication of law, the doctrine has no place here, and the Motion should be denied.

C. Plaintiffs' Breach of Express and Implied Contract Claims

This Court need not engage in a protracted analysis to conclude a contract exists: this Court previously held that Marriott's privacy policy—substantially similar to the operative one here—created an offer, and plaintiffs accepted that offer by providing PII. *Marriott MDL*, 440 F. Supp. 3d at 484. However, Plaintiffs acknowledge that under Maryland, California, and Nevada law, plaintiffs must demonstrate: 1) the existence of a valid contract; 2) breach; and 3) damages resulting from the breach. *Parkway 1046, LLC v. U.S. Home Corp.*, 961 F.3d 301, 307 (4th Cir. 2020); *Oasis West Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011); *Contreras v. Am. Fam. Mut. Ins. Co.*, 135 F. Supp. 3d 1208, 1224 (D. Nev. 2015). Plaintiffs' breach of contract claim is based on Marriott's Privacy Statement, which constitutes an objective offer to protect consumers' PII, and Plaintiffs and Class Members accepted that offer by enrolling in the loyalty program and providing their PII.

Marriott cites various inapplicable case law in an attempt to overcome this Court's well-reasoned analysis in the *Marriott MDL* based on a prior version of a privacy policy. Marriott also attempts to wordsmith and analyze the Privacy Statement *ad hoc*, but the core substance of the Court's analysis in the *Marriott MDL* remains true here: Marriott represented it would use reasonable security measures to protect Plaintiffs' and Class Members' PII, and clearly did not because—in Marriott's own words—"The data was accessed *improperly* by franchise employees." MTD at 16 n.10. While Marriott may have sought to protect the kingdom from outside intruders, it left the gates to the lion's cages wide open, permitting the lions to openly roam and hunt the inhabitants without any form of security. Marriott invited Plaintiffs and Class Members to contract for security, Plaintiffs and Class Members accepted that offer and provided their PII, and Marriott breached this contract by failing to safeguard that PII from its own employees' improper access.

The sole challenge to Plaintiffs' implied contract claim is the Parties had no "ascertainable

agreement." MTD at 17. The Court should summarily reject this argument; it starkly contradicts this Court's analysis in the *Marriott MDL*, where the terms were found for an express contract.

D. Unjust Enrichment

When an enforceable, binding agreement exists defining the rights of the parties, unjust enrichment is not available to an aggrieved party. *RaceRedi Motorsports, LLC v. Dart Machinery, Ltd.*, 640 F. Supp. 2d 660, 666 (D. Md. 2009) (quoting *Paracor Fin. v. Gen. Elec. Capital Corp.*, 96 F.3d 1151, 1167 (9th Cir. 1996)). "Rule 8(e)(2), however, permits a party to plead multiple, and when necessary, inconsistent claims." *Id.* "[W]hen the terms of a contract or parties to said contract *are disputed*, courts permit alternative pleadings." *Id.* (citations omitted). As Marriott has disputed the existence of the contracts Plaintiffs seek to enforce via the Privacy Statement, Plaintiffs "should be permitted to plead unjust enrichment in the alternative." *Id.*

Marriott's chief substantive argument is that Plaintiffs' unjust enrichment claim fails because they failed to allege what portions of their payments should have been allocated to data security, or how they would have acted differently had they known of Marriott's shoddy data security (e.g., staying elsewhere, paying less). MTD at 18. This is a familiar refrain from defendants in data breach cases and it is routinely rebuffed. *See, e.g., In re Premera Blue Cross Cust. Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1200–01 (D. Or. Aug. 1, 2016) ("Plaintiffs allege that they made payments to Premera and that under the circumstances it is unjust for Premera to retain the benefits received without payment. This is sufficient to withstand a motion to dismiss."); *see also In re: Cmty. Health Sys.*, 2016 WL 4732630, at *24 (N.D. Ala. Sep. 12, 2016) (denying motion to dismiss unjust enrichment claim in data breach case); *In re Anthem*, 2016 WL 3029783, at *28–29 (same); *Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 769–70 (W.D.N.Y.) (same). There is no requirement to plead the precise amounts attributable to data security in order to maintain an unjust enrichment claim in data breach litigation. *Ibid.*

E. Breach of Confidence

Plaintiffs acknowledge Maryland courts have declined to apply breach of confidence under substantive Maryland law. Therefore, Plaintiffs respond to Marriott's arguments lodged at their respective state-based causes of action for breach of confidence should Maryland law not apply.

1. Plaintiffs' claims under Nevada law are properly pled.

Nevada recognizes the tort of breach of confidence. *Frudden v. Pilling*, 842 F. Supp. 2d 1265, 1281 (D. Nev. 2012), *rev'd on other grounds*, 742 F.3d 1199 (9th Cir. 2014); *Perry v. Jordan*, 900 P.2d 335, 337–38 (1995). In the context of this tort, a confidential relationship arises where "one party gains the confidence of the other and purports to act or advise with the other's interests in mind." *Perry*, 900 P.2d at 338. Where a confidentiality agreement exists, a court may infer the existence of a confidential relationship. *See Atherton Resources, LLC v. Anson Resources, Ltd.*, 2019 WL 78945, at *6 (D. Nev. Jan. 2, 2019) (denying summary judgment where the parties had entered into an agreement to keep information confidential). Marriott's sole argument against Ms. Springmeyer's breach of confidence cause of action under Nevada law is that they only had a "commercial relationship, not a special relationship of confidence or anything approaching a fiduciary duty." MTD at 19. This wholly disregards the sensitive nature of consumers' PII, Marriott's representations to safeguard that PII, and Marriott's complete failure to do so.

Marriott unequivocally informs consumers (including Plaintiffs and Class Members) that it collects their PII and agrees to keep that PII out of the public realm. ¶¶ 30–35. Indeed, Marriott explicitly represents that it uses the PII to manage its "contractual relationship" with consumers, and "seek[s] to use reasonable organizational, technical and administrative measures to *protect*" consumers PII. ¶¶ 34–35. The well-pled factual allegations in the Complaint clearly demonstrate the expectation of a confidential relationship between Marriott and consumers: consumers provide PII to Marriott, Marriott accepts and stores that PII for the alleged benefit of consumers, and

Marriott promises to protect that PII from unauthorized dissemination. ¶¶ 30–35. Although the relationship between Marriott and consumers (including Plaintiffs and Class Members) does not fall within a traditional fiduciary duty recognized under Nevada law, Nevada recognizes that additional, confidential relationships may arise through interactions of parties.

2. Plaintiffs' California claims are properly pled.

Marriott's motion to dismiss the California breach of confidence claim is mistaken. Under California law, a cause of action for breach of confidence is "an obligation in law where in fact the parties made no promise. It is not based on apparent intentions of the involved parties; it is an obligation created by law for reasons of justice." *Entertainment Research Grp. v. Genesis Creative Grp.*, 122 F.3d 1211, 1227 (9th Cir. 1997) (quoting *Fink v. Goodson-Todman Enters. Ltd.*, 9 Cal.App.3d 996, 1010 (1970)). To plead such a claim, Plaintiffs must show: (i) a conveyance of confidential and novel information to the Defendant; (ii) offered to another in confidence and voluntarily received (iii) with the understanding that the information would be held in confidence; and (iv) the information was not held in confidence as contemplated. *Id.*; *San Jose Options Inc. v. Yeh*, 2014 WL 4380045, at *5 (N.D. Cal. Sept. 4, 2014). Contrary to Marriott's Motion, there is no requirement that the information be a trade secret or intellectual property. Numerous courts have held that as long as the parties understood the information was confidential, and defendant would maintain confidences but failed to do so, the claim should not be dismissed. *Yeh*, 2014 WL 4380045, at *5; *Metrano v. Fox Broad.*, 2000 WL 979664, at *6 (C.D. Cal. April 24, 2000).

Here, it is plain that Marriott understood that the PII Plaintiffs provided was confidential, and Marriott treated the PII as such as demonstrated by the fact that it did not and does not make the information publicly available to everyone as a matter of course nor share it without permission. ¶¶ 157–160. Plaintiff has adequately alleged a breach of confidence claim. Indeed, this situation is no different from others where a confidentiality obligation has been found, be it a

school, accountant, or doctor. *See Blair v. Union Free School Dist. #6*, 324 N.Y.S.2d 222, 228 (Dist. Ct. Suffolk Co. 1971) (school); *Wagenheim v. Alexander Grant & Co.*, 19 Ohio App.3d 7, 10 (Ohio 1933) (accountant); *Alberts v. Devine*, 395 Mass. 59, 69 (Ma.1985) (doctor).[9]

F. California UCL

1. Plaintiff Lopez has standing under the UCL.

To state a claim under the UCL, Plaintiffs must show they personally lost money or property "as a result of the unfair competition." *Cal. Bus. & Prof. Code* §17204; *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 330 (2011). "There are innumerable ways in which economic injury from unfair competition may be shown," including that Plaintiffs "have a present or future property interest diminished . . . be deprived of money or property to which he or she has a cognizable claim; or . . . be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Id.* at 323. Plaintiffs affirmatively pled diminished value of their personal information, consequential out-of-pocket expenses that would not have occurred save Marriott's failure to institute adequate protections of Plaintiffs' PII and/or the actual Breach, identity theft monitoring, and paying monies to Marriott for its services which Plaintiffs otherwise would not have paid had Marriott disclosed that it lacked data and cyber security practices adequate to safeguard consumers' PII from theft. ¶¶ 12, 15, 18–20, 68–69, 109. Such allegations are sufficient and actionable economic injuries under the UCL. M*arriott MDL*, 440 F. Supp. 3d at 492.

Marriott claims in its Motion that "heightened risk of identity theft, time and money spent on mitigation of that risk, and property value in one's information" all are insufficient and cites to decisions supposedly supporting that a breach of personal information was insufficient allegation

[9] Just like negligence, the duty to keep PII confidential arises separately from any contractual obligation at issue, precluding the application of the economic loss rule to the extent that the Court deems there to be such an issue. Marriott denies any contractual duty. MTD at 16–17.

of economic injury. *E.g.*, *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (dismissing diminished-value claims), *aff'd*, 572 F. App'x 494 (9th Cir. 2014); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012) (collecting cases). However, this line of authority is outdated and non-binding authority stemming from *Thompson v. Home Depot*, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007). Subsequent decisions have found Plaintiffs' allegations do support sufficient economic injury under the UCL. *In re Yahoo!*, 2017 WL 3727318, at *21; *In re Anthem*, 2016 WL 3029783, at *15. Indeed, this Court has also rejected Marriott's contentions. *Marriott MDL*, 440 F. Supp. 3d at 492. Here, Plaintiff Lopez alleges that if he knew the truth about Marriott's security practices, then he would not have stayed at Marriott or spent his money at Marriott. This is sufficient to establish standing for the UCL claim. *Id.*; *see Kwikset*, 246 P.3d at 885–86 (economic injury established where plaintiff "surrender[s] in a transaction more, or acquire[s] in a transaction less, than he or she otherwise would have")." Thus, contrary to Marriott's position, Plaintiff alleges injuries sufficient for a UCL claim.

2. Plaintiff's allegations satisfy all prongs of the UCL.

Furthermore, Plaintiff states a claim under all prongs of the UCL. The UCL provides a cause of action for practices that are: (i) unlawful; (ii) unfair; ***or*** (iii) fraudulent. *Cal. Bus. & Prof. Code* §§ 17200, *et seq.* "The UCL's coverage is sweeping, and its standard for wrongful business conduct intentionally broad." *Moore v. Apple Inc.*, 73 F. Supp. 3d 1191, 1204 (N.D. Cal. 2014). Each prong provides a "separate and distinct theory of liability." *Lozano v. AT&T Wireless Services Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Marriott's motion must be denied because Plaintiffs pled at least one variety of unfair competition under California law.

As Marriott's acknowledges, the UCL "borrows violations of other laws and treats them as unlawful practices' that the unfair competition law makes independently actionable." *Cel-Tech*

Commc'ns, Inc. v. L.A. Cellular Tel. Co., 20 Cal.4th 163, 180 (1999). Thus, "anything that can properly be called a business practice and that at the same time is forbidden by law" states a claim. *Id.* As Marriott admits, here Plaintiff alleges violations of *Cal. Civ. Code* § 1798.81.5(b) and *Cal. Civ. Code* § 1798.82. However, Marriott fails to address the alleged violations of the FTC Act, ¶¶ 48–53, and its publications, which can likewise satisfy the unlawful prong. Thus, these unlawful business practices state a UCL claim regardless of Marriott's arguments concerning *Cal. Civ. Code* § 1798.81.5(b) and *Cal. Civ. Code* § 1798.82. The well-pled violations of these laws require denial of Marriott's Motion on the UCL claim, just as the Court did in the *Marriott MDL*.

Furthermore, Marriott is wrong that *Cal. Civ. Code* § 1798.81.5(b) and *Cal. Civ. Code* § 1798.82 have no application here. First, Lopez does allege his name, address, email address, account information, and other highly personal details including credit card information were held and stored by Marriott. ¶ 31. Moreover, Marriott itself has said that it cannot, at least not yet, rule out the possibility that credit card information, passport numbers, or driver's license information were improperly accessed. ¶ 23. It is objectively reasonable, at the pleading stage, to accept such information has been accessed—indeed, Marriott's action of offering credit monitoring to the customers whose data was breached indicates that a reasonable and prudent person would presume that such access to confidential information had been accomplished.

Additionally, contrary to Marriott's contention, it is a question of fact (not law) whether one month and 5 days is sufficiently "expedient" notice to Plaintiffs to satisfy the requirement that Marriott provide disclosures of the Breach to Plaintiffs in the most expedient time possible and without unreasonable delay, along with taking the measures necessary to determine the scope of the Breach and restore the reasonable integrity of the data system, which has not yet occurred as the internal investigation is ongoing, as required under *Cal. Civ. Code* § 1798.82. Therefore, this issue cannot be resolved on a motion to dismiss.

The "unfair" prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal.4th 1134, 1143 (2003). Now Marriott suggests the test of the "unfair" prong must either "be tethered to some legislatively declared policy or have some effect on competition," or be "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." This is misplaced. Under California law there are three possible tests defining unfair. *Drum v. San Fernando Valley Bar Ass'n*, 182 Cal.App.4th 247, 257 (2010). The first is the tethering test. Second, is the balancing test which asks whether the practice is "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." The third test requires "(1) that the consumer injury be substantial; (2) that the injury not be outweighed by any countervailing benefits to consumers or competition; and (3) the injury is one that consumers could not have reasonably avoided." *Id.*

Plaintiffs have adequately alleged all three tests of "unfair." First, the California legislature has affirmed a policy and enacted legislation designed to protect PII and punish those who fail to safeguard adequately against data breaches. *See, e.g.*, *Cal. Civ. Code* § 1798.81.5(b) and *Cal. Civ. Code* § 1798.82. In fact, the FTC Act likewise provides that the public policy of the United States is to safeguard against data breaches. Additionally, Plaintiffs have alleged that Marriott promised in its Privacy Statement to protect customer's data, and yet Marriott failed to safeguard this data. ¶ 122. Plaintiffs likewise allege that Marriott's shortcomings violated various laws, including the FTC Act, all of which seek to protect consumer data and ensure that entities entrusted with this information use appropriate security measures. ¶ 53. Plaintiffs also allege that Marriott deceived the public into believing their data was safe when it was not. ¶ 35. Lastly, Plaintiffs allege the injury to consumers is substantial insofar as diminution in value, actual costs of credit monitoring, or freezes that stem from the real threat of identity theft the Breach caused, and is not one which the customer could not have avoided. ¶¶ 109, 116, 128, 136, 165, 177, 183. Such allegations, taken

separately or plainly when taken together, state a UCL claim under the "unfair" prong. *See e.g.*, *In re Anthem,* 162 F. Supp. 3d at 990; *In re: Adobe*, 66 F. Supp. 3d at 1227.[10]

G. Plaintiffs Allegations Support A CCPA Claim

The CCPA states, in relevant part: "Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action." *Cal. Civ. Code* § 1798.150(a). Marriott contends the CCPA has no application here because it only applies to "personal information" as defined in § 1798.81.5(d)(A)(1), which Marriott contends "is not at issue here." MTD at 21–22. As explained above, Lopez has sufficiently alleged personal information, as defined in *Cal. Civ. Code* § 1798.81.5, is at issue.

Marriott also argues Lopez failed to provide notice of this claim, as is allegedly required. MTD at 23. Marriott, however, is mistaken that "30 days' written notice identifying the specific provisions . . . the consumer alleges have been or are being violated." MTD at 23 (citing *Cal. Civ. Code* § 1798.150). Indeed, as Marriott admits, Lopez is an individual consumer who thus may initiate a claim here "solely for actual pecuniary damages without providing notice." *Cal. Civ. Code* § 1798.150(b). Contrary to Marriott's arguments, Lopez has alleged pecuniary damage; he alleges, *inter alia*, that he paid Marriott money for its services which he would not have, had Marriott disclosed that it lacked data and cyber security practices adequate to safeguard his PII. (¶ 20.) Thus, Marriott's Motion must be denied.

[10] Any argument that the "balancing test" weighs in Marriott's favor is misplaced as it is a factual determination and premature. *In re Anthem*, 162 F. Supp. 3d at 990; *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1073 (N.D. Cal 2012).

H. Springmeyer Sufficiently Pled a Claim Under Nevada's DTPA

The thrust of Marriott's attack against Springmeyer's Nevada DTPA claim is that it lacks sufficient detail under Rule 9(b). Springmeyer meets the Rule 9(b) standard by alleging the "time, place, and content" required by Rule 9(b). *Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776, 784 (4th Cir. 1999). First, Springmeyer identifies the pertinent details of Marriott's misrepresentations that its data and cyber security practices were adequate. *See* ¶ 30 (noting the effective date of the Privacy Statement as June 3, 2019, which was in effect at the time of the Breach). Springmeyer also identifies the content of Marriott's hollow promise to protect customer's data and subsequent failure to do so. ¶ 122. Springmeyer further alleges that Marriott represents it would use consumers' PII to "manage [its] contractual relationship" with consumers, but deceived the public into believing their data was safe when it was not and instead was available to franchise employees in a foreign country. ¶¶ 34–36.

In a familiar refrain, Marriott suggests Springmeyer should know precisely what data and cyber security policies were in place, how they were inadequate, or what alternatives would have prevented the Breach. MTD at 24. Although Springmeyer does not have access to the passwords and model numbers of Marriott's servers, the policies and permissions for employees, or other likely confidential and trade secret information, Springmeyer sufficiently pleads with Rule 9(b) detail that Marriott's data and cyber security systems were so poor, lax, and ineffective that a Russian franchise employee had access to a Nevada resident's PII, despite Marriott's affirmations that the PII would be used for "contractual purposes" to manage its relationship with Springmeyer. Clearly, Marriott represented it would safeguard consumers' PII, but instead Marriott's poor, lax, and ineffective data and cyber security granted at least two Russian franchise employees access to the PII of at least 5.2 million consumers. Springmeyer has met the Rule 9(b) standard.

I. Declaratory Judgment

Marriott argues that Plaintiffs' Declaratory Judgment claim for relief fails if Plaintiffs' substantive claims fail, and is duplicative of other claims. MTD at 24. Plaintiffs have plausibly alleged their substantive claims, and therefore the Court should reject Marriott's first argument. Plaintiffs' claims are also not duplicative: the Declaratory Judgment claim seeks a declaration that Marriott "continues to breach [its] legal duties by failing to employ reasonable measures to secure consumers' PII," and prospective injunctive relief requiring Marriott "to employ adequate security protocols consistent with law and industry standards to protect consumers' PII." ¶¶ 154(c), 155. Marriott has alleged in conclusory fashion, under non-binding law, that the Declaratory Judgment is somehow a "tack-on claim," MTD at 25, n.16, despite the unique relief requested therein.

III. A Nationwide Class is Appropriate

For the reasons argued above, Maryland law applies to Plaintiffs' and all Class Members' claims sounding in tort and contract. *Supra*, II.A. True, the subclasses Plaintiffs seek to represent are necessarily limited to their respective states, and the Plaintiffs may not represent a class of Maryland consumers under, *e.g.*, Maryland's consumer statutes, but nothing forecloses Plaintiffs from seeking redress on behalf of the nationwide class of consumers aggrieved by the Breach based on application of Maryland law via *lex loci contractus* and *lex loci delicti*.

CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that the Court deny Marriott's Motion in its entirety. If the Motion is granted in any way, Plaintiffs request the opportunity to amend their complaint to cure any pleading deficiencies. Fed. R. Civ. P. 15.

Dated: September 4, 2020

/s/ John A. Yanchunis

MURPHY, FALCON & MURPHY, P.A.
William H. Murphy III, Esq. (Bar No. 30126)
hassan.murphy@murphyfalcon.com
One South Street, 23rd Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen Hanson Riebel (*pro hac vice*)
khriebel@locklaw.com
Kate M. Baxter-Kauf (*pro hac vice*)
kmbaxter-kauf@locklaw.com
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

GLANCY, PRONGAY & MURRAY
Brian Murray
BMurray@Glancylaw.com
230 Park Avenue, Suite 530
New York, NY 10169
Telephone: (212) 682-5340
Facsimile: (212) 884-0988

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis (*pro hac vice*)
jyanchunis@ForThePeople.com
Jean S. Martin (*pro hac vice*)
jeanmartin@ForThePeople.com
Ryan J. McGee (*pro hac vice*)
rmcgee@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

TOSTRUD LAW GROUP, P.C.
Jon A. Tostrud (*pro hac vice*)
jtostrud@tostrudlaw.com
Anthony M. Carter (*pro hac vice*)
acarter@tostrudlaw.com
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Facsimile: (310) 278-2640

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2020, the foregoing was filed with the Clerk of Court using CM/ECF, which will send notification to the registered attorneys of record that the document has been filed and is available for viewing and downloading.